REMARKS

Claims 1-4, 8-10, 12-14, 19, 26-29, 33-35, 37-39, 42 and 43 are pending in the present application. Claims 1, 9, 10, 12, 13, 19, 26, 33-35, 37, 38, 42 and 43 have been amended, and Claims 5, 11, 17, 18, 30, 36 and 44 have been cancelled, herewith. Reconsideration of the claims is respectfully requested.

Amendments were made to the specification to correct errors and to clarify the specification. No new matter has been added by any of the amendments to the specification.

I. Objection to Specification

The Examiner objected to the Specification, stating that the use of JAVA should be capitalized and accompanied by generic terminology. Applicants have amended the Specification at page 8 to capitalize JAVA and provide generic terminology. Therefore, the objection to the Specification has been overcome.

II. Objection to Claims

The Examiner objected to Claims 11 and 36, stating that such claims are a substantial duplicate of Claims 1 and 26, respectively, and would be improper under 37 CFR 1.75 if Claims 1 and 36 were allowed. Applicants have cancelled Claims 11 and 36 herewith, without prejudice or disclaimer, in order that this case may expeditiously pass to issue. Therefore, the objection to the claims has been overcome.

III. 35 U.S.C. § 102, Anticipation

The Examiner rejected Claims 1-5, 8-14, 17-19, 26-30, 33-39 and 42-44 under 35 U.S.C. § 102 as being anticipated by US Patent 5,778,072 to Samar. This rejection is respectfully traversed.

With respect to Claim 1, such claim has been amended to recite "wherein the key is a software key and the selected process is the hardware process and further comprising converting the software key into a hardware form useable by the hardware process for performing the cryptographic operation". As can be seen per Claim 1, the key that is

used in an encryption of data is a software key *that is converted to a hardware form* useable by the hardware process for performing cryptographic operations. The cited reference does not teach any type of key conversion at all. Rather, the cited reference teaches use of either a smartcard or a software process for performing a cryptographic operation, based upon whether a smartcard is present (Figure 2, blocks 205, 207 and 221). If a smartcard is present, the user is authenticated by initiating a challenge/response protocol, or a particular password/personal identification number protocol, with the user's smartcard (col. 6, lines 6-11; Figure 2, blocks 207 and 135). The smart card will return a value to the operating system indicating whether the authentication was successful (col. 6, lines 17-19). There is no type of key conversion in this process, as *the key is secretly maintained within the smartcard* such that it cannot be externally accessed (col. 6, lines 50-54). If a smartcard is not present in the system, the user is authenticated with any of the selected encryption services 129 (col. 6, lines 36-38). Since in this scenario no smartcard is present, the key store manager requests (from the selected encryption service) a private key for the user. This private key is written to the user information file (col. 6, lines 40-46). In this scenario of no smartcard being present, there also is no type of key conversion of a software key into a hardware form usable by the hardware process, as this scenario describes use of a software key by a software process. Quite simply, there is no teaching of converting a software key into a hardware form useable by a hardware process for performing a cryptographic operation.

For the encryption operation described at col. 7, lines 10-44, the data to be encrypted is passed to the smartcard where it is encrypted using a "non-readably stored key" (col. 7, lines 30-31), such that the user's private key is never exposed outside the card (col. 7, lines 37-44). Again, there is no type of key conversion performed, as the cited reference is keen on maintaining a preexisting hardware encryption key internal to the smartcard, which is not readable or otherwise accessible outside the card. The passage cited at col. 8 does not describe any type of key conversion, but instead describes use of either a public key or a private key to decrypt data. These public/private keys are not converted from one form to another.

It is thus urged that Claim 1 is not anticipated by the cited reference, as every element of the claimed invention is not identically shown in a single reference.

Applicants traverse the rejection of Claims 2-4 and 19 for reasons given above with respect to Claim 1 (of which Claims 2-4 and 19 depend upon).

With respect to Claim 8, such claim recites performing the cryptographic operation using the selected process, wherein the cryptographic operation is an encryption of data using a key, wherein the key is a hardware key and the selected process is the software process and further comprising converting the hardware key into a software form useable by the software process for performing the cryptographic operation. As described above with respect to Claim 1, the cited reference does not teach any type of key conversion from one form to another, and in fact the reference is keen on not allowing hardware keys to be used with or accessed by other types of cryptographic operations due to security concerns (col. 6, lines 50-54; col. 7, lines 37-44). It is thus urged that Claim 8 is not anticipated by the cited reference, as every element of the claimed invention is not identically shown in a single reference.

Applicants traverse the rejection of Claims 9 and 10 for similar reasons to those given above with respect to Claim 8 (of which Claims 9 and 10 depend upon).

Applicants traverse the rejection of Claim 26 (and dependent Claims 27-29 and 44) and 43 for similar reasons to those given above with respect to Claim 1.

Applicants traverse the rejection of Claim 33 (and dependent Claims 34, 35 and 37-39) and 42 for similar reasons to those given above with respect to Claim 8.

Therefore, the rejection of Claims 1-5, 8-14, 17-19, 26-30, 33-39 and 42-44 under 35 U.S.C. § 102 has been overcome.

IV. Conclusion

It is respectfully urged that the subject application is patentable over the cited reference and is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: 6/15/05

Respectfully submitted,

Cathrine K. Kinslow
Reg. No. 51,886
Wayne P. Bailey
Reg. No. 34,289
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorneys for Applicants